PX129

Expert rebuttal report of Stephen McKeon, Ph.D.

In response to expert reports by:

Patrick B. Doody (12/20/19)

Carmen A. Taveras (12/20/19)

Maurice P. Herlihy (12/27/19)

January 10, 2020

Securities and Exchange Commission v. Telegram Group Inc. and TON Issuer Inc

TABLE OF CONTENTS

I. ASSIGNMENT

1. I have been retained by the law firm, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP ("Counsel"), counsel for Telegram Group Inc. and TON Issuer Inc (the "Defendants") in the matter of *Securities and Exchange Commission v. Telegram Group Inc. and TON Issuer Inc*. Counsel has asked me to review and respond to the analysis and conclusions contained in the following expert reports submitted by the U.S. Securities and Exchange Commission ("SEC"): (1) the Expert Report of Patrick B. Doody ("Mr. Doody") dated December 20, 2019 ("Doody Report); (2) the Expert Report of Carmen A. Taveras, Ph.D. ("Dr. Taveras") dated December 20, 2019 ("Taveras Report"); and (3) the Expert Report of Maurice P. Herlihy ("Dr. Herlihy") dated December 27, 2019 ("Herlihy Report") (collectively, "Opposing Reports").

2. I wrote the Expert Report of Stephen B. McKeon, Ph.D., for this matter dated December 27, 2019, which I refer to at various points of this rebuttal report as "my report" or "McKeon Report". My qualifications and the documents that I reviewed are detailed in my report. Any additional documents that I reviewed since my report are listed in Appendix A.

3. All opinions are my own. I respectfully reserve the right to supplement, change, or modify my conclusions and summary of opinions, if additional information becomes available.

4. I am being compensated at $850 per hour in this matter. My compensation is not dependent on reaching certain opinions or the outcome of this litigation.

II. SUMMARY OF OPINIONS

5. The Opposing Reports focus a great deal of attention on the expectations of Round 1 and Round 2 private placement purchasers ("Early Purchasers") who entered into contracts which provided for the future delivery of Grams if the TON blockchain was completed and launched. The Round 1 and Round 2 purchase contracts were structured as private placements

exempt from Federal securities laws. My opinion is that the expectations of the Earlier Purchasers differ substantially from those who may purchase Grams after the blockchain is launched.[1] The Early Purchasers likely expected to profit from their purchase of Grams, but in exchange for that expectation they assume the risk that the TON Blockchain would not launch or would not be successful upon launch. I review evidence on the risk inherent to early purchases and economic outcomes for comparable assets in Section III (A).

6. The Doody Report and Taveras Report argue that the pricing formula and price stabilization function described in the January 2018 version of the TON White Paper[2] imply that Gram purchasers were being promised guaranteed investment profits and protection from losses. The price of Grams specified by the reference price formula ("Reference Price") in the TON White Paper, however, is not the same as the market price for Grams at the time of anticipated launch. As such, my opinion is that discounts relative to the Reference Price are not representative of expected economic outcomes for Early Purchasers of Grams, and Early Purchasers are not guaranteed investment profits. The evidence and analysis supporting this opinion are provided in Section III (B).

7. My opinion is that the Doody Report contains unsupported statements regarding the expected consumptive uses for Grams at the time of the anticipated mainnet launch. The available evidence supports numerous consumptive uses for Grams, as detailed in my report and reviewed in Section III (C). Consumptive uses include both services within the TON ecosystem, which are expected to be live at the time of the anticipated mainnet launch, as well as third-party developmental efforts for applications and services. Further, it should be expected that third-party

[1] A mainnet launch typically refers to when a blockchain project opens to the public, which usually follows development and testing.
[2] Unless otherwise noted, all references to the "TON White Paper" refer to the March 2, 2019 version.

applications and services developers will drive their own engagement, independent of Telegram's efforts, because they will have an economic incentive to do so.

8. My opinion is that both the Doody Report and Herlihy Report make unsupported statements regarding the factors that would be considered by prospective purchasers of Grams. For example, factors such as theft prevention and banking relationships are outside the scope of what would be expected from the base layer protocol and are typically addressed by third-party applications and services. Further, Mr. Doody cites evidence from a report on factors considered by venture capital equity investors, which are distinct from factors considered by purchasers of decentralized cryptoassets. Mr. Doody's evidence on the high correlation of cryptoasset returns points to aggregate market forces as a meaningful component of expected returns, and profits derived from these market forces would be independent from the efforts of Telegram.

9. Furthermore, Dr. Herlihy states that prudent purchasers would not allocate capital to blockchain assets without a security analysis and audit.[3] This statement is directly contradicted by the evidence of billions of dollars of market capitalization for cryptoassets on competing blockchains prior to security audits, as well as the $1.7 billion in purchases by Early Purchasers of Grams, many of whom are sophisticated institutional investors. I review the evidence and analysis behind this opinion in Section III (D).

10. My opinion is that the empirical analysis in the Taveras Report contains numerous flaws and cannot be relied upon. Specifically, several of the comparable assets used are fundamentally different than Grams, the time series of prices used in the analysis is not comparable to the market conditions facing Grams at the time of the anticipated mainnet launch, and the interpretation of regression coefficients is inaccurate. These factors result in the analysis

[3] Herlihy Report, Paragraph 35.

containing no relevant information content. The evidence and analysis supporting this opinion is found in Section III (E).

III. RESPONSES TO EXPERT OPINIONS AND ANALYSIS

A. The Profit Expectations of Early Purchasers is Independent from, and Not Relevant to, the Expectations of Prospective Purchasers Following the Anticipated Mainnet Launch

11. The Doody Report and Taveras Report rely on the outdated January 2018 TON White Paper[4] which has since been superseded by the March 2019 White Paper and the recent public notice made by TON[5] ("Public Notice"). Some of the features they discuss, including discretion of the TON Foundation and TON Reserve to buy Grams on the open market to stabilize prices, have been eliminated. Prospective purchasers following the anticipated mainnet launch would be expected to rely on all public information available at the time of purchase. In my experience, this is true whether they intend to purchase for consumptive reasons or speculative investment.

12. Nonetheless, the Doody Report and Taveras Report focus heavily on the profit expectations of the Early Purchasers, whose purchase decisions were made based on circumstances existing and information available in early 2018. Pre-launch purchasers of cryptoassets who fund the development of a platform typically do expect to earn profits post-launch, but they bear substantial risks including the execution risk that the launch might fail. Thus, the price they are willing to pay is substantially lower than the price that might be expected in post-launch public trading. Further, their expectations of profit are distinct from expectations of post-launch purchasers because post-launch purchasers face a different risk profile for the asset once the

[4] Doody Report, Paragraph 6; Taveras Report, Paragraph 23.
[5] See: https://telegram.org/blog/ton-gram-notice

platform is live. I was informed by counsel that these purchase contracts were exempt from Federal securities laws by Regulation D and Regulation S.

13. Early Purchasers face execution risk, which is the uncertainty that the platform will be successfully developed and launched. Further, Round 1 purchasers are subject to risks induced by post-launch price volatility that occurs prior to the expiration of their lock-up period. Post-launch purchasers face reduced execution risk when the platform is live and operational, and they are not subject to lock ups that prohibit exit. Additionally, live networks have more functionality and economic uses, therefore, additional demand for tokens is likely to increase the price.

14. The risk related to price volatility during the lock-up period can be substantial, for example, Algorand, which is a competing Proof of Stake ("PoS") blockchain, launched on June 19, 2019 at $2.44 per ALGO token, and traded as high as $3.57 in the days afterwards. However, 30 days after launch, the price had dropped to $0.68 and declined further to $0.32, 90 days after launch.[6] Pre-launch purchasers that were locked up during this period had no opportunity to sell at the price observed around the time of launch. In other cases, Early Purchasers of cryptoassets are rewarded for bearing the substantial risk. An example is Ethereum, which initially sold units of Ether for $0.31 in July and August 2014. When the first "production release," called Homestead, was launched in March 2016 the price of Ether had risen to $12.50.[7]

15. Mr. Doody states that the Reference Price was "novel" due to the fact that the price of Grams increased "exponentially" as they were issued. I note that this is not uncommon in prior cryptoasset issuances, and in fact, the recent examples identified in Appendix B are a few among many where the cryptoassets were sold in multiple issuances with the price consistently increasing

[6] See: https://messari.io/asset/algorand
[7] See: https://blog.sfox.com/from-crowdfunded-blockchain-to-ico-machine-an-ethereum-price-history-ddb31c3134c4

in each issuance by hundreds or thousands of percent. The increase in price is not surprising since Early Purchasers accept more risk than later purchasers, because with each succeeding round, the project moves further in its development phase and closer to launch.

B. Early Purchasers in Grams are Not Guaranteed Investment Profits

16. In the TON White Paper, a reference price formula dictated the price paid by Early Purchasers.[8] Effectively, as more Grams (or contracts for Grams) are issued, the Reference Price increases at an exponential rate. Hence, Round 1 Purchasers paid a lower price than Round 2 Purchasers for the contracts that would distribute Grams, following the anticipated mainnet launch.

17. It was originally contemplated in the TON White Paper that the Reference Price mechanism would also be used subsequent to the anticipated mainnet launch to endow the TON Foundation through the TON Reserve with the right, but not the obligation, to buy Grams when the market price dropped below 50% of the Reference Price, or issue Grams when the market price exceeded the Reference Price, thereby generating a mechanism to mitigate price volatility within these bounds. However, the purchase provision was subsequently eliminated[9], a fact that is ignored by the opposing reports, which invalidates any analysis around the repurchase function. Additionally, Telegram has since announced that it is under no obligation, and makes no promise or commitment, to ever establish a TON Foundation or similar entity in the future.[10]

---

[8] TON White Paper, p. 128-129.

[9] Telegram Group Inc. Fourth Supplemental Memorandum to the Staff of the SEC (July 25, 2019), p. 2:

> "The TON Foundation's role will be limited to the following three activities: (1) selling Grams through the TON Reserve and utilizing the proceeds from any sales of Grams from the TON Reserve in the manner described below; (2) awarding Grams from the Incentives Pool in the manner described below; and (3) publishing non-binding opinions and research results regarding the TON Blockchain's development and policy (similar to the Ethereum Foundation)."

[10] See: https://telegram.org/blog/ton-gram-notice

18. He further states "the Reference Price formula works in such a way that both the First and Second Round Initial Purchasers will be guaranteed a profit if the market price of Grams tanks after launch and the Ton Reserve implements its buyback program at the buyback price dictated by the Reference Price formula."[11] This is an inaccurate and unsupported representation for several reasons.

19. First, as noted above, the purchase provision had been eliminated by the time of Mr. Doody's report, a fact that is ignored.

20. Second, Mr. Doody glosses over the fact that the purchasing function was described as discretionary and not a legal obligation on the part of Telegram or the TON Foundation.[12] Early Purchasers had no contractual right to effectuate a buyback of their Grams and thus wouldn't have relied upon it as a guarantee or credible signal. Moreover, Telegram never guaranteed any profits to Early Purchasers and instead unambiguously informed them that their investment "may decrease in value over time and/or lose all monetary value". [13]

21. Finally, as detailed below in my analysis of the Taveras Report, the numbers simply don't add up to support the notion that the TON Reserve would possess the resources to guarantee a profit, or even a return of capital, to Early Purchasers.

22. Dr. Taveras calculates "the profits that Gram investors could expect to realize if the TON Reserve buys back Grams at its Maximum Purchase Price (half of the Reference Price) shortly after launch, assuming that the price of Grams falls and stays below half of the Reference Price."[14] Dr. Taveras calculates a profit of $11,689,801 accruing to Early Purchasers, however this result is obtained by TON Reserve spending $12 million more than the total amount raised in

[11] Doody Report, Paragraph 43.
[12] TON White Paper, p. 129-130.
[13] Purchase Agreement for Grams (TG-001-00000020), p. 11.
[14] Taveras Report, Paragraph 32.

order to generate these profits. No reasonable buyer would expect TON Reserve to possess more capital than was initially raised under the assumption that the price of Grams falls and stays below half of the Reference Price after launch.

23. Both Mr. Doody and Dr. Taveras are confusing the resources of Telegram, the TON Foundation and TON Reserve. The TON Foundation was contemplated to be capitalized with only $5M[15] and the TON Reserve is anticipated to be capitalized solely with Grams.[16] Yet both Mr. Doody and Dr. Taveras assume that, if immediately upon launch of the TON Blockchain the price of Grams sufficiently declined, the TON Reserve would purchase all of the Grams allocated to the Early Purchasers and provide them with a small profit.[17] However, neither Mr. Doody nor Dr. Taveras explain where the capital for these repurchases would come from or why the Early Purchasers would expect their entire investment to be repurchased with a profit when they had been given substantial discounts to assume the additional risks described. In fact, Dr. Taveras explicitly states that only $1.4 billion of the original $1.7 billion raised in the private placements would be available to support buying activities and, even then, does not explain why Gram buyers would expect those funds would be available to the TON Foundation or TON Reserve or the source of the additional capital that would be needed to support the purchases.[18]

24. Further, Mr. Doody claims in his report that the very existence of the buyback feature, which he fails again to note has been eliminated,[19] sends a "clear message that Telegram intends to spend its own capital, if necessary, to lower the risk and increase the expectation of profit from the purchase of its Grams."[20] This would imply not only that the TON Foundation

[15] Telegram Group Inc. Second Supplemental Memorandum to the Staff of the SEC (February 27, 2018), p. 6.
[16] Telegram Group Inc. Second Supplemental Memorandum to the Staff of the SEC (February 27, 2018), p. 4.
[17] Doody Report, Paragraphs 45-46.
[18] Taveras Report, Paragraph 34.
[19] Simos, Elias "The Current State of Telegram Open Network: A sleeping giant awakens." October 2019, p. 18-19. See: https://drive.google.com/file/d/1PCEypWk6Z4QLdyvhXm1CRk79pQ0Zkbkp/view
[20] Doody Report, Paragraph 40.

would exercise its discretion to use the Gram purchase function but also that Telegram itself would contribute funds for the buybacks. However, Mr. Doody provides no explanation or justification for this statement. He acknowledges that there is no contractual obligation to make such purchases. And neither he nor Dr. Taveras identify a contractual obligation for Telegram to provide its own capital for the purchases or any economic incentive for Telegram to do so. Moreover, Mr. Doody's supposition that Gram buyers would expect the TON Foundation to operate to protect their profit expectations ignores that the TON Foundation was also contemplated to have discretion to *sell* Grams to avoid upward spikes in Gram prices, which would tend to curb profit expectations.

25. There is further evidence of flawed logic in the juxtaposition of the analysis of price stability and expectations of Early Purchasers in the Opposing Reports. Specifically, both Mr. Doody and Dr. Taveras conclude that the contemplated open market operations of the TON Foundation would be unable to stabilize the price of Grams,[21] therefore, it would (under this logic) follow that purchasers shouldn't reasonably expect that the TON Foundation would exercise its option to purchase Grams or that it would have the incentive to do so.

26. More broadly, I emphasize that Mr. Doody's and Dr. Taveras' focus on discounts relative to the anticipated Reference Price at mainnet launch is misplaced. Dr. Taveras states "The market price of Grams will be given by demand and supply and need not be close to or correlated with the Reference Price."[22] Therefore, it is not clear whether the price paid by Early Purchasers represents a substantial discount to the price at which they may ultimately sell the asset after launch, but what is clear is that any discount relative to the Reference Price is not representative of an expected economic outcome for Gram holders.

[21] Doody Report, Paragraph 48; Taveras Report, Paragraphs 37-39, 43.
[22] Taveras Report, Paragraph 22.

27. In summary, the opposing experts attempt to establish a built-in guarantee of profits by Early Purchasers, but there is no evidence supporting this claim. In my experience, pre-launch purchasers of cryptoassets do not expect any guarantee of their profits or even a return of their investment. In fact, they understand that they are taking the risk that they will lose potentially all of their investment. Further, as a signal to future purchasers, Telegram states in the Public Notice: "you should NOT expect any profits based on your purchase or holding of Grams, and Telegram makes no promises that you will make any profits."[23]

C. Errors in Statements About Commercial Uses

28. Mr. Doody states "There appear to be only minimal commercial uses for Grams anticipated at launch. For example, no major vendor to my knowledge has agreed to accept Grams as a form of payment."[24] However, the statement lacks basis and is contradicted by the wealth of information contained in Telegram investor materials, its White Paper[25] and Primer,[26] as well as its submissions to the SEC,[27] which describe in detail a comprehensive stack of commercial services that would be available to the TON user base at launch.

29. His report further ignores the completion status updates from Telegram which show that, as of January 28, 2019, the TON Virtual Machine components driving the execution of smart contracts, various TON services and decentralized applications, were 95% complete, most TON Network components were 100% complete and TON Blockchain Block Generation and Validation components were 50-95% complete. Furthermore, the Doody Report also ignores TON's

[23] See: https://telegram.org/blog/ton-gram-notice
[24] Doody Report, Paragraph 9.
[25] TON White Paper, p. 3-4.
[26] 2018 Stage A Primer (TG-003-00000056), p. 9-10.
[27] Defendants' Responses and Objections to Plaintiff's First Set of Interrogatories, No. 5, *SEC v. Telegram, et al.*, No. 19-cv-9439(PKC) (S.D.N.Y. Nov. 22, 2019).

November 22, 2019 submission to the SEC which identified the work on TON DNS, TON Payments and TON Services had already been completed, and the development of TON Storage and TON Proxy was near complete and expected to be ready by the launch of the mainnet.[28] Therefore, most TON components are complete or nearing their completion and will be fully available to the TON blockchain users at the launch of the mainnet.[29]

30. The Doody Report also ignores the availability of fully functional commercial uses for test Grams available on the TON testnet, for example, Button Wallet, or fully developed applications which will be available at the time of the launch of the TON blockchain, for example, TON Wallet.[30] I note that Exhibit 4 of my report lists numerous expected commercial uses for Grams, which are above and beyond the rich suite of services available internally within TON. Further, later in his report Mr. Doody points to an important category of non-investment economic uses, gas and transaction fees, which constitute the purchase of compute power and are therefore a consumptive use of Grams.[31]

31. There is also a dearth of support for Mr. Doody's statements regarding the efforts required of Telegram to drive adoption of consumptive uses of Grams. Specifically, Mr. Doody states "it is worth noting that the second set of products, which require integration with Telegram Messenger, would need significant development and maintenance efforts by Telegram Messenger to ensure i) proper usage and engagement by Telegram Messenger users and ii) the subsequent usage and engagement of the TON Blockchain by those users."[32]

---

[28] Defendants' Responses and Objections to Plaintiff's First Set of Interrogatories, Nos. 2 and 5, *SEC v. Telegram, et al.*, No. 19-cv-9439(PKC) (S.D.N.Y. Nov. 22, 2019); McKeon Report, Paragraphs 137-138.
[29] TON Development Status (January 28, 2019).
[30] Defendants' Responses and Objections to Plaintiff's First Set of Interrogatories, Nos. 5, *SEC v. Telegram, et al.*, No. 19-cv-9439(PKC) (S.D.N.Y. Nov. 22, 2019).
[31] Doody Report, Paragraph 30.
[32] Doody Report, Paragraph 31.

32. From an economic standpoint, I note that engagement by Messenger users is not solely dependent on Telegram. As rational economic actors, third-party developers are anticipated to act to benefit their own economic gain from their applications. They would therefore make their own efforts to drive user engagement for their products, through the Telegram Messenger or independent of Telegram, similar to the way developers of applications on Ethereum don't rely on the Ethereum Foundation to drive engagement for their products and services. Mr. Doody identifies no evidence that suggests these third-party developers would need to rely on the efforts of Telegram to support their products after the mainnet launch. In fact, Telegram states in the Public Notice "Telegram won't be obligated to maintain the platform or create any apps for it. It's possible we never will."[33]

D. Factors Considered by Prospective Purchasers

33. Both Mr. Doody and Dr. Herlihy make inaccurate and unsupported statements regarding the factors that would likely be considered by prospective purchasers of Grams.

34. Mr. Doody states "a reasonable person or entity considering the purchase of Grams to purchase goods and services would look to a number of different factors that received little or no attention in Telegram's promotional material, including fraud prevention, theft, integration with their existing banking relationships, and compliance with financial regulations."[34] At the same time, Mr. Doody points to the lack of any disclosure of "professional experience in finance or banking" on the Telegram team.[35] Thus, Mr. Doody appears to acknowledge that Gram purchasers would expect to benefit from the efforts of third-party developers creating additional functionality rather than the efforts of Telegram. Further, Howell et al. (2019) find that issuer teams having

[33] See: https://telegram.org/blog/ton-gram-notice
[34] Doody Report, Paragraph 8.
[35] Doody Report, Paragraph 24.

financial backgrounds is not a consistent statistically significant predictor of a blockchain's success or failure.

35. In my opinion, there is very little support for Mr. Doody's assertion that the factors he identifies are actually important to consumptive users or, even if they are, that those factors are not addressed in the TON White Paper. Specifically:

a. **Fraud prevention** is a key feature of blockchains. A distributed ledger acts as a source of truth regarding valid transactions as a product of the architecture of the consensus mechanism. As such, fraud prevention is addressed heavily in, and is in fact the primary focus of the TON White Paper in the sense that the document provides technical details on transaction validation.[36] Fraud prevention is one of the primary value propositions for consumptive uses of cryptoassets like Grams, because alternative forms of digital payments such as credit cards are subject to billions of dollars of fraud annually, the majority of which is remote payment, such as payments made over the internet.[37]

b. **Theft**: As with all digital assets, theft prevention is the responsibility of the holder. None of the major base layer protocols such as Bitcoin or Ethereum make guarantees about theft prevention. Holders of these assets maintain their own operational security procedures and look to custody providers and wallets to provide additional solutions to prevent theft.

c. **Banking relationships** are not the responsibility of the blockchain software protocol. Integration with the banking system is executed through third-party fiat

[36] TON White Paper, p. 44-74.
[37] See: https://www.federalreserve.gov/publications/files/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf

on-ramps such as a trading venue like Coinbase, or TON Labs' integration with Wirecard, which are covered on page 24 of my report. Additionally, most decentralized applications don't require banking relationships at all. Payments within gaming, social media, advertisements, prediction markets, and many others are all executed in the native cryptoasset.

d. **Compliance with regulations**: Telegram executed Reg D and Reg S filings for the pre-sale, which is more than other protocols such as Ethereum did prior to launch. Additionally, according to the Interrogatories, "Defendants further respond that they undertook know-your-customer ("KYC") and anti-money laundering ("AML") processes with respect to all private placement purchasers." From an economic standpoint, my opinion is that these actions constitute a best effort in terms of regulatory compliance. Furthermore, it is not clear specifically which regulations Mr. Doody is referring to or why consumptive users would care or be subject to these regulations.

36. Mr. Doody later states, "I believe that a reasonable purchaser of Grams would consider the following factors when purchasing Grams: company and staff credentials, addressable market, product, market dynamics, and investor terms and investment exit."[38] The evidence Mr. Doody uses to support this statement is Roberts and Barley (2005), which is a series of interviews with venture investors in 2004.

37. There are at least three problems with the application of this evidence to an analysis of Grams. First, the interviewees are institutional venture investors, who may bear resemblance

[38] Doody Report, Paragraph 22.

to Early Purchasers, but would not necessarily speak to the investment criteria of post-launch purchasers.

38. Second, the interviewees are commenting on the factors that led to their venture investments in the late 1990's and early 2000's, but a lot has changed in the technology landscape over the past 15 years. For example, this period pre-dated the rise of networks like Facebook, which altered the way venture investors think about network effects.

39. Finally, and most importantly, these factors are applicable to investments in early stage equity, not cryptoassets. As emphasized on page 11 of my report, decentralized networks are not corporations and investments in cryptocurrencies are not analogous to investments in equity. With regards to purchasers in the post-launch period, the academic literature cited in my report, such as Cong et al (2019), suggest that cryptoasset purchasers are more interested in developer activity and network functionality than the factors cited in the 2005 report by Roberts and Barley. Furthermore, standard terms that are present in early stage equity, such as liquidation preference or pro rata rights, simply do not exist in decentralized cryptoassets, so terms are rarely a defining criterion for investment in cryptoassets. Finally, investor exit is not a strong consideration since the assets are typically publicly traded at the time of purchase, post-launch.

40. Mr. Doody states "Telegram's position as a popular forum for promoting digital asset investments would not particularly matter to somebody deciding whether to buy and hold Grams as a personal or business decision to fulfill a functional need regarding cash management or payments solutions."[39] The evidence that contradicts this statement can be found in the list of consumptive use applications in Section IX of my report. Many of the payment solutions, such as wallets, that will utilize Grams are natively digital and could integrate with Messenger, or, for

[39] Doody Report, Paragraph 26.

example, in the case of Button Wallet and ParJar are already integrated with Messenger. Further, the native TON Wallet will not be integrated with Messenger at the time of the anticipated launch. Specifically, Telegram states: "At the time of the anticipated launch of the TON Blockchain, Telegram's TON Wallet application is expected to be made available solely on a stand-alone basis and will not be integrated with the Telegram Messenger service."[40]

41. Purchasers of cryptoassets would be expected to place higher weight on the ability of the blockchain to perform the essential service: processing transactions in a decentralized manner that is resistant to corruption of the ledger. Decentralization, coupled with scalability, leads to the factors such as functionality and network effects that scholars such as Cong et al (2019) have shown to be determinants of value. Relatedly, it is worth noting that Dr. Herlihy reports that 36 validators were detected on the TON testnet.[41] While this is lower than the 100 validators expected at the anticipated launch of TON, it is nonetheless more decentralized than other PoS blockchains like EOS, which has only 21 validators.[42]

42. Mr. Doody states "In my opinion, a reasonable purchaser of Grams would consider the large scale of this potential market [the market for payments] and the potential for the TON Blockchain to achieve mass-market adoption as a reason to purchase Grams with the expectation of profits derived from the efforts of the Telegram team to develop the TON Blockchain."[43] While the potential market size and adoption rates are relevant to purchasers, the efforts of Telegram are not necessarily related to these factors. As described in more detail in Sections VIII and IX of my report, third-party developer efforts will be very important for consumer adoption, and Mr. Doody's observation that the Telegram's offering materials did not identify its team's finance and

[40] See: https://telegram.org/blog/ton-gram-notice
[41] Herlihy Report, Paragraph 33.
[42] See: https://iang.org/papers/EOS_An_Introduction-BLACK-EDITION.pdf ; McKeon Report, Paragraph 182.
[43] Doody Report, Paragraph 29.

banking experience indicates that they are not marketing themselves as being qualified to develop applications that require this expertise.

43. Another factor that points to profit expectations that are independent from the efforts of Telegram is the evidence Mr. Doody's cites on the high correlation of returns to cryptoassets (Hu et al, 2018).[44] This evidence is consistent with the analysis in my report suggesting that aggregate market movements, known as systematic returns, are a large portion of the total return expected to accrue to assets such as Grams.[45]

44. Turning to Dr. Herlihy's report, he states the following economic opinion: "no prudent investor or consumer would trust their assets to such a system without a thorough security analysis and audit."[46] The economic evidence suggests otherwise. Specifically, a review of the history of blockchain security audits by leading security audit service providers, such as OpenZeppelin, reveals that market participants routinely trust their assets to blockchain protocols and applications in advance of security audits. For example, OpenZeppelin conducted a security audit on the Solidity compiler and language for the Ethereum Foundation.[47] This was the first publicly available security audit sponsored by the Ethereum Foundation to my knowledge.[48] It was published on November 1, 2018, several years after Ethereum's public launch.[49] Ethereum had a market capitalization of $20.5 billion on the date of the report. Additionally, there is no evidence that Block.one has publicly released a security audit of the EOSIO blockchain and yet the aggregate market capitalization of EOS is approximately $2.3 billion as of January 2, 2020. Many of the market participants who invested in Ether or EOS in the absence of a security audit

[44] See: http://webuser.bus.umich.edu/urajan/research/crypto.pdf
[45] McKeon Report, Paragraphs 209-215.
[46] Herlihy Report, Paragraph 35.
[47] See: https://docs.google.com/document/d/1PZBSCBWBwd6AqWCgXqLnw8FNQ4HRurP5usrXuKuU0a0/edit
[48] I am also aware of audits on smart contracts built on top of Ethereum, and of a July 2018 audit of "Casper".
[49] See: https://media.consensys.net/a-short-history-of-ethereum-a8fdc5b4362c

are sophisticated institutional investors with fiduciary duties, and often generated substantial returns from these investments. Lastly, the Early Purchasers at issue here have already expended hundreds of millions of dollars for the right to receive Grams upon launch. Taken together these facts cast doubt on the assertion that they were acting imprudently.

45. In many cases, security audits are conducted independently by third parties, well after a blockchain has launched. Recent examples include:

a. An article dated August 13, 2019 by researchers from the University of Texas at San Antonio and the US Air Force Research Laboratory, which investigates vulnerabilities of Ethereum at the application layer, the data layer, consensus layer, network layer and the Ethereum environment.[50]

b. In 2019, the Korea Advanced Institute of Science and Technology published an article on the potential vulnerabilities of the EOS.IO blockchain. Based on the results, the paper outlines four potential attacks, stemming for the unique characteristics of EOS.IO, one of which may in fact "disrupt the essential function of its blockchain and incapacitate the entire EOS.IO system."[51] The article was published one year after the official launch of the EOS.IO network.[52]

c. In April 2019, the Korea Advanced Institute of Science and Technology published an article outlining potential vulnerabilities of the Stellar blockchain. The researchers investigated the degree of the network's centralization and determined how centralization can have a negative impact on the system, namely through the failure of a few validators. The results of the study indicate that "the nodes in

[50] See: https://arxiv.org/pdf/1908.04507.pdf
[51] See: https://www.usenix.org/system/files/woot19-paper_lee.pdf
[52] See: https://block.one/news/eosio-1-0-release/

> Stellar cannot run SCP [Stellar Consensus Protocol] if only two nodes fail."[53] The article was released approximately 4 years after the network's launch.[54]

46. I note that one of the primary features of public blockchains is that they are designed to be resilient to adversarial participants. This is known as Byzantine Fault Tolerance, whereby the primary function of the network—posting valid transactions to the ledger—is robust to malicious actors. As such, they are distinct from closed source proprietary platforms where the user must rely on security analysis by a single operator. Public open source blockchains are routinely attacked, as well as audited and analyzed, by third parties, thereby shifting the task of security analysis and audits to the community rather than solely on the progenitor.

E. The Empirical Analysis of Dr. Taveras' Report is Flawed and Cannot be Relied Upon

47. The market price simulations and empirical analysis of the Taveras Report are severely flawed by the choice of (i) comparable assets, (ii) time periods of the price series, and (iii) interpretation of regression coefficients.[55]

48. While some of the assets used in Dr. Taveras' analysis have features similar to Grams, as described in my report, several do not. For example, the most extreme negative returns are observed for Paragon and Dragon Coins, both of which are ERC20 tokens issued on top of the Ethereum blockchain, and neither is a blockchain protocol cryptocurrency like Gram. They are both targeted towards specific industry use cases, cannabis in the case of Paragon, and gambling in the case of Dragon Coin. According to an SEC press release, Paragon raised $12 million through

[53] See: https://arxiv.org/pdf/1904.13302.pdf
[54] See: https://sci.smithandcrown.com/projects/stellar
[55] Taveras Report, Paragraphs 40-50.

an ICO, used in part to buy a physical co-working space for cannabis start-ups.[56] Dragon Coin issued a press release announcing that they raised $320 million with the use of funds primarily geared towards building a physical floating casino in Macau.[57] Bancor, another comparable used by Dr. Taveras, is also an Ethereum token rather than a native asset for a base layer blockchain protocol like Grams. Suffice to say, these assets do not bear much resemblance to Grams and their use in the empirical analysis is misguided.

49. Turning to the other six comparables from Exhibits 6 and 7 in the Taveras Report (Bitcoin, Ethereum, XRP, Bitcoin Cash, EOS, and Tezos), they are native assets for base layer protocols, which makes them good candidates, but the circumstances around their histories make large segments of the time series of prices inappropriate for comparable analysis. I summarize the issues with each below:

a. **Bitcoin**: In terms of historical economic price analysis, Bitcoin really has no comparable. As the first cryptocurrency to exist, it had no economic value at creation. Dr. Taveras' price series begins in July 2010. To put this era in perspective, the first recorded use of bitcoin in a transaction for goods or services occurred in May 2010 when Laszlo Hanyecz bought two pizzas for 10,000 Bitcoins (the equivalent of over $82 million at today's prices).[58] There was effectively no infrastructure in place for cryptocurrency at that time, which makes Bitcoin an inadequate comparable for price series analysis because the market for

[56] See: https://www.sec.gov/news/press-release/2018-264 for ICO proceeds and CoinMarketCap.com for market capitalization.
[57] See: https://cointelegraph.com/press-releases/dragon-coins-public-token-sale-is-open
[58] See: https://qz.com/1285209/bitcoin-pizza-day-2018-eight-years-ago-someone-bought-two-pizzas-with-bitcoinsnow-worth-82-million/

cryptocurrencies that an asset like Grams faces today bears almost no resemblance to the early era of Bitcoin.

b. **Ethereum** bears many similarities to TON, but like Bitcoin it was the first of its kind. In Ethereum's case it was the first smart contract platform. Moreover, the time series analysis begins in August 2015, which is prior to Homestead, the first "production release" of the platform in March 2016.[59]

c. **XRP** also had early beginnings, the price series starts in 2013, so the market was much less developed compared to today. Plus, the architecture of XRP doesn't resemble Grams in that XRP is a private, centralized blockchain whereas TON is a public, decentralized blockchain. It follows that the market may not price these assets in the same way.

d. **Bitcoin Cash** is unique in that it was the first major fork of Bitcoin[60], and considerable debate existed regarding how to value it.

e. This leaves **EOS** and **Tezos**, which are the most similar to Grams in that they are both smart contract platforms that raised capital in order to develop their platform and launched in the relatively recent past. However, they differ in the sense that both executed public ICOs before the blockchain was live, so early trading is not representative of the price dynamics Grams will face if trading begins in conjunction with a live and fully functional platform.

50. In addition to the factors listed above, the price data Dr. Taveras used contains the period of extreme volatility in late 2017 and early 2018, which may be an anomaly and not

[59] See: https://consensys.net/blog/blockchain-explained/a-short-history-of-ethereum/
[60] See: https://www.bloomberg.com/news/articles/2018-09-18/bitcoin-cash-s-survival-in-question-as-possible-split-looms

representative of future market dynamics. In sum, the price data used by Dr. Taveras is not representative of the market conditions likely to face purchasers of Grams.

51. To illustrate the difference in calibration parameters, I obtained price data from Coin Metrics for the three closest comparables to TON/Grams: Ethereum, EOS, and Tezos, over the period from their mainnet launch to January 2, 2020. The simple mean daily return over these periods is -0.47% for EOS, -0.24% for Tezos, and 0.07% for Ether. The equal weighted average daily return of these three is 0.21%, roughly an order of magnitude lower than the 2.0% upper bound assumption in Dr. Taveras' analysis.

52. Finally, prior research has documented at least two features of cryptoasset returns that violate assumptions underlying Dr. Taveras' use of Geometric Brownian Motion (GBM) in her simulation analysis. The first is periods of volatility clustering (Othman et al., 2019). Hence it incorrect to assume constant sigma, as it is more accurately modelled as time varying. The second is that log returns of cryptoassets violate the normality assumption in GBM. Cryptoasset log returns exhibit "fat tails," meaning a higher frequency of extreme returns, relative to what would be expected under a normal distribution.

53. Without any empirically established justification, Dr. Taveras assumes that the dynamics of cryptocurrency prices and returns is the same as for publicly traded equities and, as the result, applies the standard geometric random walk model to estimate the mean and standard deviation of daily returns of cryptocurrencies contained in her dataset. On the one hand, it is well known that daily stock returns sometimes violate the assumptions embedded in the geometric random walk model to the extent that they are not independent across periods and identically distributed, exhibit autocorrelation, as well as periods of volatility clustering. On the other hand, there is a body of accumulated empirical evidence demonstrating that cryptocurrency returns are

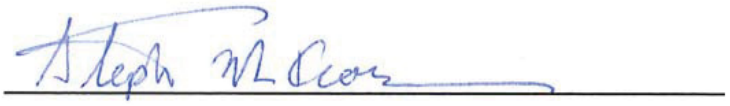
anything but normally distributed and, therefore, violate the very basic condition under which the geometric random walk model would be valid.

54. These issues, taken together with the problems in comparables described above, support my opinion is that the empirical analysis lacks relevant information content and cannot be relied upon.

* * * * * * * * *

Respectfully submitted,

Dated: January 10, 2020



Stephen McKeon, Ph.D.

Appendix A: Documents Relied Upon

Case-Related Documents

Expert Report of Maurice P. Herlihy (Dec. 27, 2019)

Expert Report of Patrick B. Doody (Dec. 20, 2019)

Expert Report of Carmen A. Taveras (Dec. 20, 2019)

Other Documents

EOS – An Introduction (Jul. 5, 2017)

Academic Publications

Kim, Minjeong, Yujin Kwon, and Yongdae Kim. "Is Stellar as Secure As You Think?" In Proceedings of the IEEE Security & Privacy on the Blockchain, 2019.

Lee, Sangsup, Daejun Kim, Dongkwan Kim, Sooel Son, and Yongdae Kim. "Who Spent My EOS? On the (In)Security of Resource Management of EOS.IO." In WOOT '19: Proceeding of the 13th Conference on Offensive Technologies. (pp. 13), 2019.

Chen, Huashan, Marcus Pendleton, Laurent Nijilla, and Shouhuai Xu. "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses." arXiv preprint arXiv:1908.04507, 2019.

Roberts, M. J., & Barley, L., How venture capitalists evaluate potential venture opportunities, Harvard Business School Research and Ideas, May 2005.

Hu, Albert S., Christine A. Parlour, and Uday Rajan. "Cryptocurrencies: Stylized Fats on a New Investible Instrument." Working paper University of California Berkeley, 2018.

Othman, A.H.A., Alhabshi, S.M. and Haron, R., 2019. The effect of symmetric and asymmetric information on volatility structure of crypto-currency markets: A case study of bitcoin currency. Journal of Financial Economic Policy.

Appendix B: Prices During Cryptoasset Issuances

Entity	Date	Reported Price	% Δ in Price[1]	Reported Amount Raised	Current Market Cap[2]
Hedera Hashgraph	Issuance 1: Q1 – Q2 2017[3] Issuance 2: March 13, 2018[4] Issuance 3: August 1, 2018[5]	$.0035[6] $.005-$.006[6] $.096-$.12[6]	 ↑57% ↑1864%	$3M[6] $18M[4] $104M[7]	$20M
EOS	Issuance 1: June 26 – 30, 2017[8] Issuance 2: July 1, 2017 – June 1, 2018[9]	$.86[8] $4.42[8]	 ↑414%	$4.1B[10]	$2.6B
Filecoin	Issuance 1: August 2017[11] Issuance 2: August 10 -September 7, 2017[12]	$.75[11] $1.30-$4.68[13]	 ↑299%	$52M[11] $205M[12]	Not listed
Polkadot	Issuance 1: October 2017[14] Issuance 2: Q2 2019[15]	$30[16] $120[16]	 ↑300%	$145M[17] $60M[15]	Not listed

[1] Percent change in price calculated based on either the midpoint or average prices, if applicable
[2] Market cap is as of January 9, 2020 from https://coinmarketcap.com/all/views/all/
[3] See: https://www.hedera.com/about
[4] See: https://www.hedera.com/blog/we-have-launched-our-crowd-sale
[5] See: https://medium.com/hashgraph/we-have-launched-our-crowdsale-faq-a55c2f09e676
[6] See: https://hbarprice.com/hbar-coin-release/
[7] See: https://www.crowdfundinsider.com/2018/09/138822-hedera-hashgraph-files-form-d-with-sec-reports-104-million-raised-in-saft-offering/
[8] See: https://bravenewcoin.com/insights/eos-price-analysis-us2-6b-already-raised-in-ongoing-ico
[9] See: https://media.consensys.net/a-retrospective-of-the-eos-token-sale-172d3437932b
[10] See: https://www.coindesk.com/the-first-yearlong-ico-for-eos-raised-4-billion-the-second-just-2-8-million
[11] See: https://techcrunch.com/2017/08/10/filecoins-ico-opens-today-for-accredited-investors-after-raising-52m-from-advisers/
[12] See: https://www.coindesk.com/257-million-filecoin-breaks-time-record-ico-funding
[13] https://www.wsj.com/articles/latest-hot-digital-coin-offering-187-millionin-one-hourfor-filecoin-1502481514
[14] See: https://techcrunch.com/2017/10/17/polkadot-passes-the-140m-mark-for-its-fund-raise-to-link-private-and-public-blockchains/
[15] See: https://cointelegraph.com/news/blockchain-protocol-polkadot-sells-500-000-of-its-tokens-price-still-unspecified
[16] See: https://cointelegraph.com/news/polkadot-tokens-sold-on-secondary-markets-at-discounted-rates-report
[17] See: https://www.coindesk.com/ethereum-co-founders-polkadot-closes-token-sale-claiming-1-2-billion-valuation